JOURNAL OF NUMBER THEORY 2, 404–413 (1970)

Class Numbers of Algebraic Number Fields of Eisenstein Type

MAKOTO ISHIDA

Department of Mathematics, Tokyo Metropolitan University, Setagaya, Tokyo, Japan

Communicated by P. Roquette

Received January 21, 1969; revised October 15, 1969

It is proved that, for a non-Galois algebraic number field K of odd prime degree ℓ, the class number of K is divisible by ℓ, provided a rational prime number $p \equiv 1 \pmod{\ell}$ ramifies completely in K. Also it is shown that, for $K = \mathbf{Q}(a^{1/n})$ with rational prime numbers $p_1, p_2, \ldots, p_s$ such that $p_i^{e_i} \| a$ and $(e_i, n) = 1$, the class number of K is divisible by $\prod_{i=1}^{s}(p_i - 1, n)$, provided n is odd. A similar result is shown for the case of even n.

In this paper, we shall investigate class number factor in an algebraic number field with a completely ramifying rational prime number. Such an algebraic number field will be said to be of Eisenstein type because, as shown in **1**, it is obtained by adjoining to $\mathbf{Q}$ a root of an Eisenstein polynomial with respect to that prime number. We give in **2** some elementary results on such algebraic number fields. Then first in **3** we prove that for a non-Galois algebraic number field K of odd prime degree ℓ, if a rational prime number p with $p \equiv 1 \pmod{\ell}$ ramifies completely in K (i.e., K is of Eisenstein type with respect to such p), then K has an unramified cyclic extension of degree ℓ and so the class number h_K of K is divisible by ℓ. Secondly in **4** we consider a pure algebraic number field $K = \mathbf{Q}(a^{1/n})$ with rational prime numbers $p_1, p_2, \ldots, p_s$ such that $p_i^{e_i} \| a$ and $(e_i, n) = 1$ (in this case, K is of Eisenstein type with respect to each of $p_1, p_2, \ldots, p_s$) and prove that: if n is odd, then the class number h_K of K is divisible by $\prod_{i=1}^{s}(p_i - 1, n)$[1]; and if n is even, then h_K is divisible by $\prod_{i=1}^{s} t_i/(2, t_i)$, where $2t_i = (p_i - 1, 2n)$. Similar results are also given for subfields of pure algebraic number fields.

1. Let K be an algebraic number field of degree n over $\mathbf{Q}$. We say that K is *of Eisenstein type* with respect to a rational prime number p, if

[1] A similar result for the case $n = \ell^{\nu}(\ell = \text{odd prime})$ was shown in A. FRÖLICH, The genus field and genus group in finite number fields II, *Mathematika* **6** (1959), 142–146.

K is obtained by adjoining, to $\mathbf{Q}$, a root α of an Eisenstein polynomial with respect to p; that is, there is an element α of K such that $K = \mathbf{Q}(\alpha)$ and the minimal polynomial of α is

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \tag{1}$$

with $a_i \in \mathbf{Z}$, $p \mid a_i$ $(1 \leqslant i \leqslant n)$ and $p \parallel a_n$. Then we easily see that

$$(p) = \mathfrak{p}^n \text{ in } K \text{ and } \mathfrak{p} \parallel \alpha, \tag{2}$$

where $\mathfrak{p}$ is a prime ideal of K.

So, if K (of degree n) is of Eisenstein type with respect to each one of rational prime numbers $p_1, p_2, \ldots, p_s$, then we have

$$(p_1) = \mathfrak{p}_1^n, (p_2) = \mathfrak{p}_2^n, \ldots, (p_s) = \mathfrak{p}_s^n \text{ in } K.$$

Conversely, suppose that for an algebraic number field K of degree n, we have $(p_1) = \mathfrak{p}_1^n, (p_2) = \mathfrak{p}_2^n, \ldots, (p_s) = \mathfrak{p}_s^n$ in K, where p_i are rational prime numbers and $\mathfrak{p}_i$ are prime ideals in K. Then there exists an integer α in K such that $\mathfrak{p}_j \parallel \alpha$ $(1 \leqslant j \leqslant s)$ and we see easily that $K = \mathbf{Q}(\alpha)$. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ $(a_i \in \mathbf{Z})$ be the minimal polynomial of α over $\mathbf{Q}$. As $(p_j) = \mathfrak{p}_j^n$ in K, we have

$$f(X) \equiv (X - t_j)^n \pmod{p_j} \quad \text{with } t_j \in \mathbf{Z};$$

and so $p_j \mid a_1, p_j \mid a_2, \ldots, p_j \mid a_n$. Comparing the maximal exponent of $\mathfrak{p}_j$ in each term of $f(\alpha) = 0$, we have $p_j \parallel a_n$, which implies that $f(X)$ is an Eisenstein polynomial with respect to each one of $p_1, p_2, \ldots, p_s$. Hence K is of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$.

Therefore we have the following

PROPOSITION. *For an algebraic number field K of degree n over $\mathbf{Q}$, the following three assertions are equivalent.*

(1) *K is of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$.*

(2) *We have $(p_1) = \mathfrak{p}_1^n, (p_2) = \mathfrak{p}_2^n, \ldots, (p_s) = \mathfrak{p}_s^n$ in K.*

(3) *K is obtained by adjoining, to $\mathbf{Q}$, a root of an Eisenstein polynomial with respect to each one of $p_1, p_2, \ldots, p_s$.*

COROLLARY. *If K is of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$, then so is any subfield of K.*

2. Now we prove two easy lemmas on an algebraic number field K of Eisenstein type with respect to p. Let $[K : \mathbf{Q}] = n$ and $K = \mathbf{Q}(\alpha)$, where (1) is the minimal polynomial of α over $\mathbf{Q}$. Let $\mathfrak{O}_K$ be the ring of integers in K

LEMMA 1. *We have*

$$p \nmid (\mathfrak{O}_K : \mathbf{Z}[\alpha]).^2 \tag{3}$$

Proof. Suppose that $p \mid (\mathfrak{O}_K : \mathbf{Z}[\alpha])$. Then there exists an element ω of $\mathfrak{O}_K$ such that $\omega \notin \mathbf{Z}[\alpha]$ but $p\omega \in \mathbf{Z}[\alpha]$. Writing $p\omega = x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}$ $(x_i \in \mathbf{Z})$, we have, by (2),

$$\begin{aligned} p\omega = \sum_{i=0}^{n-1} x_i\alpha^i \equiv 0 \pmod{(p) = \mathfrak{p}^n} &\Rightarrow x_0 \equiv 0 \pmod{\mathfrak{p}} \\ &\Rightarrow x_0 \equiv 0 \pmod{(p) = \mathfrak{p}^n} \Rightarrow \sum_{i=1}^{n-1} x_i\alpha^i \equiv 0 \pmod{\mathfrak{p}^n} \\ &\Rightarrow x_1\alpha \equiv 0 \pmod{\mathfrak{p}^2} \Rightarrow x_1 \equiv 0 \pmod{\mathfrak{p}} \\ &\Rightarrow x_1 \equiv 0 \pmod{(p) = \mathfrak{p}^n} \Rightarrow \cdots \Rightarrow x_{n-1} \equiv 0 \pmod{(p)}. \end{aligned}$$

Consequently we have $\omega = \sum_{i=0}^{n-1} (x_i/p)\,\alpha^i \in \mathbf{Z}[\alpha]$, which is a contradiction.

LEMMA 2. *For an element $\gamma \in \mathfrak{O}_K$, we have*

$$N_{K/\mathbf{Q}}(\gamma) \equiv x^n \pmod{p} \tag{4}$$

with some $x \in \mathbf{Z}$.

Proof. Denoting $k = (\mathfrak{O}_K : \mathbf{Z}[\alpha])$, we have $p \nmid k$ by (3) and $k\gamma \in \mathbf{Z}[\alpha]$, i.e., $k\gamma = \sum_{i=0}^{n-1} x_i\alpha^i$ $(x_i \in \mathbf{Z})$. Note that $-a_1, a_2, \ldots, (-1)^n a_n$ (a_i = coefficients of $f(X)$ in (1)) are fundamental symmetric polynomials of all the conjugates of α over $\mathbf{Q}$. So, since we have $N_{K/\mathbf{Q}}(k\gamma) = k^n N_{K/\mathbf{Q}}(\gamma) = x_0^n + \{\mathbf{Z}\text{-linear combination of } a_1, a_2, \ldots, a_n\}$ and $p \mid a_i$ $(1 \leqslant i \leqslant n)$, we have $k^n N_{K/\mathbf{Q}}(\gamma) \equiv x_0^n \pmod{p}$, which implies (4) by (3).

Clearly Lemma 2 implies that the norm mapping $N_{K/\mathbf{Q}}$ defines a homomorphism of the ideal class group C_K of K into the factor group of the multiplicative group $\mathfrak{G}$ of $\mathbf{Z}/(q)$ modulo $\pm\mathfrak{G}^n$. So we have the following result by assuming that $p \equiv 1 \pmod{2n}$: Suppose that there exists a rational prime number q satisfying

[2] By this, we mean the index of the submodule $\mathbf{Z}[\alpha]$ in the module $\mathfrak{O}_K$.

(1) q is a primitive root modulo p,

(2) q has a prime divisor $\mathfrak{q}$ of degree 1 in K, i.e., $N_{K/\mathbf{Q}}(\mathfrak{q}) = q$.

Let m be the order of the ideal class of $\mathfrak{q}$ in C_K. Then we have $\mathfrak{q}^m = (\gamma)$ with some $\gamma \in \mathfrak{O}_K$ and so, by Lemma 2, $q^m = N_{K/\mathbf{Q}}(\mathfrak{q}^m) = |N_{K/\mathbf{Q}}(\gamma)| = \pm x^n \pmod p$. As $(p-1)/n$ is even, we have $q^{m(p-1)/n} \equiv 1 \pmod p$. As q is a primitive root modulo p, m/n must be in $\mathbf{Z}$, i.e., $n \mid m$. Hence we can conclude that C_K has an element of order n and so h_K is divisible by n. We use these arguments in the last section. As a remark, in the case where n is odd, we need only to assume that $p \equiv 1 \pmod n$ in the above arguments.

EXAMPLE. For a given natural number n, let p be a rational prime number such that $p \equiv 1 \pmod{2n}$ and q a rational prime number which is a primitive root modulo p. Let K be an algebraic number field, of degree n, of Eisenstein type with respect to p and q (for example, $K = \mathbf{Q}((pq)^{1/n})$). Then q ramifies completely in K and so q has a prime divisor of degree 1 in K. So, C_K has an element of order n and h_K is divisible by n.

3. For a natural number m, we denote by ζ_m a primitive m-th root of unity.

THEOREM 1. *Let K be an algebraic number field of odd prime degree ℓ, which is of Eisenstein type with respect to a rational prime number p with*

$$p \equiv 1 \pmod \ell \tag{5}$$

and is not contained in $\mathbf{Q}(\zeta_p)$. Let k be the (unique) subfield[3] of $\mathbf{Q}(\zeta_p)$ of degree ℓ over $\mathbf{Q}$. Then $L = K \cdot k$ is an unramified cyclic extension of K, of degree ℓ, and so the class number h_K of K is divisible by ℓ.

Proof. Let K^* be the smallest Galois extension, over $\mathbf{Q}$, containing K. Then $G_1 = \mathrm{Gal}(K^*/\mathbf{Q})$ is isomorphic to a subgroup of S_ℓ (the symmetric group of ℓ letters) and we have $\ell \mid \#(G_1)$ and $\#(G_1) \nmid \ell!$. On the other hand, $G_2 = \mathrm{Gal}(k/\mathbf{Q})$ is cyclic and of order ℓ. Let $L = K \cdot k$ and $\Omega = K^* \cdot k = K^* \cdot L$. Then we see easily that L/K is a cyclic extension of degree ℓ and Ω/K^* is also a cyclic extension of degree ℓ. Since ℓ is odd, L/K is unramified with respect to all the infinite prime divisors of K. So we have to prove that L/K is unramified with respect to all the finite prime divisors of K.

(a) Let $\mathfrak{p}^*$ be a prime divisor of p in K^* and e^* the ramification index of $\mathfrak{p}^*$ in $K^*/\mathbf{Q}$. Then, as p ramifies completely in K and $e^* \mid [K^* : \mathbf{Q}] = \#(G_1)$, we have $\ell \mid e^*$ and $p \nmid e^*$. Hence the inertia group T^* of $\mathfrak{p}^*$ in $K^*/\mathbf{Q}$ is

[3] We have $k = \mathbf{Q}(\zeta_p^{r^\ell} + \zeta_p^{r^{2\ell}} + \cdots + \zeta_p^{r^{(p-1/\ell)\ell}})$, where r is a primitive root modulo p.

cyclic and of order e^* with $\ell \mid e^*$. However, as $G_1 = \mathrm{Gal}(K^*/\mathbf{Q})$ is isomorphic to a subgroup of S_ℓ, if the order of an element of G_1 is divisible by ℓ then it must be ℓ. So we see that $e^* = \ell$ and so $\mathfrak{p}^*$ is unramified in K^*/K.

(b) Suppose that a prime divisor $\mathfrak{P}$ of p in Ω ramifies in Ω/K^*. Then the ramification index e of $\mathfrak{P}$ in $\Omega/\mathbf{Q}$ is ℓ^2 by (a) and so $p \nmid e$. So the inertia group T of $\mathfrak{P}$ in $\Omega/\mathbf{Q}$ is cyclic and of order ℓ^2. However $\mathrm{Gal}(\Omega/\mathbf{Q}) \cong G_1 \times G_2$ has no element of order ℓ^2. Hence $\mathfrak{P}$ is unramified in Ω/K^*.

(c) Let $\mathfrak{P}_0$ be a prime divisor of p in L. Then a prime divisor $\mathfrak{P}$ of $\mathfrak{P}_0$ in Ω is unramified in Ω/K by (a) and (b) and so $\mathfrak{P}_0$ is unramified in L/K. Since p is the only ramifying rational prime number in $k/\mathbf{Q}$, we see that L/K is unramified with respect to all the finite prime divisors of K. Thus the proof is completed.

COROLLARY. *Let K be an algebraic number field of odd prime degree ℓ, which is of Eisenstein type with respect to s rational prime numbers p_1, $p_2, \ldots, p_s$ with $p_i \equiv 1 \pmod{\ell}$ and is not contained in $\mathbf{Q}(\zeta_{p_1 p_2 \cdots p_s})$. Then K has an unramified abelian extension of degree ℓ^s and so h_K is divisible by ℓ^s.*

Remark 1. In Theorem 1, the assumption $K \not\subset \mathbf{Q}(\zeta_p)$ is always satisfied, provided K has one of the following properties:

(1) $K/\mathbf{Q}$ is not a Galois extension.

(2) There is another rational prime number $q \neq p$ ramifying in K.

On the other hand, this assumption is necessary for our conclusion. For example, we know that $K = \mathbf{Q}(\alpha)$ with $\alpha^3 - 7\alpha + 7 = 0$ has the class number 1.

Remark 2. We can give another proof of Theorem 1 for $\ell = 3$ (the divisibility of h_K by 3) by the method stated in **2**. We give a sketch of it. Let K be a non-Galois, cubic number field of Eisenstein type with respect to p. We may take, without loss of generality, an element α of K such that $K = \mathbf{Q}(\alpha)$ and the minimal polynomial $f(X) = X^3 - aX + b$ of α is an Eisenstein polynomial with respect to p. Then the smallest Galois extension K^*, over $\mathbf{Q}$, containing K contains a unique quadratic number field $K_0 = \mathbf{Q}((4a^3 - 27b^2)^{1/2})$. It is easily proved that if a rational prime number q ($q \nmid 4a^3 - 27b^2$) remains prime in K then $\left(\frac{4a^3 - 27b^2}{q}\right) = 1$. So, taking a rational prime number q such that

(1) $q \nmid 4a^3 - 27b^2$,

(2) $\left(\frac{4a^3 - 27b^2}{q}\right) = -1$,

(3) q is a primitive root modulo p,

we see that q has a prime divisor of degree 1 in K. Hence if $p \equiv 1 \pmod 3$, we have $3 \mid h_K$ by the similar reasoning in the end of **2**.

4. Let K be a pure algebraic number field, i.e., $K = \mathbf{Q}(a^{1/n})$ with $a \in \mathbf{Z}$. Let us suppose that there are rational prime numbers $p_1, p_2, \ldots, p_s$ such that

$$p_i^{e_i} \| a \qquad \text{with} \quad (e_i, n) = 1. \tag{6}$$

LEMMA 3. *The field K is of degree n and is of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$, i.e., we have $(p_i) = \mathfrak{p}_i^n$ in K $(1 \leqslant i \leqslant s)$.*

Proof. Let $\mathfrak{p}_i$ be a prime divisor of p_i in K. Let $\mathfrak{p}_i^u \| a^{1/n}$ and $\mathfrak{p}_i^v \| p_i$. Then, by (6), we have $nu = e_i v$ and $(e_i, n) = 1$, which imply $n \mid v \leqslant [K : \mathbf{Q}] \leqslant n$. So we have $n = [K : \mathbf{Q}]$ and $(p_i) = \mathfrak{p}_i^n$.

In the following, we use the above notations and we fix a primitive root r_i modulo p_i for $1 \leqslant i \leqslant s$.

A. *The Case of Odd n*

Let $t_i = (p_i - 1, n)$ for $1 \leqslant i \leqslant s$. As seen later[4], we may suppose that all p_i's are odd. Then we can take prime numbers $q_1, q_2, \ldots, q_s$ such that

$$\begin{aligned} &q_i \nmid na, \qquad (q_i - 1, n) = 1, \\ &q_i \equiv r_i \pmod{p_i}, \\ &q_i \equiv r_j^{t_j} \pmod{p_j} \qquad \text{for} \quad j \neq i. \end{aligned} \tag{7}$$

In fact, we can find such a q_i in the arithmetic progression defined by

$$\begin{aligned} &q_i \equiv r_i \pmod{p_i}, \\ &q_i \equiv r_j^{t_j} \pmod{p_j} \qquad \text{for} \quad j \neq i, \\ &q_i \equiv 2 \pmod{p} \text{ for prime divisors } p \text{ of } n \ (\neq p_1, \ldots, p_s). \end{aligned}$$

Here we note that, as n is odd and $p_j - 1$ is even, $t_j = (p_j - 1, n) < p_j - 1$ and so $r_j^{t_j} \not\equiv 1 \pmod{p_j}$. Now, since, by $(q_i - 1, n) = 1$, the mapping $x \to x^n$ defines an automorphism of the multiplicative group of $\mathbf{Z}/(q_i)$, the polynomial $X^n - a \pmod{q_i}$ has a root in $\mathbf{Z}/(q_i)$. So, by $q_i \nmid na$, there is a prime divisor $\mathfrak{q}_i$ of q_i, of degree 1, in K. Let $\mathfrak{C}_i$ be the ideal class of $\mathfrak{q}_i$ in the ideal class group C_K of K. Suppose that we have

$$\mathfrak{C}_1^{a_1} \mathfrak{C}_2^{a_2} \cdots \mathfrak{C}_s^{a_s} = 1 \text{ in } C_K.$$

[4] See Remark after Theorem 2.

Then we have $\mathfrak{q}_1^{a_1}\mathfrak{q}_2^{a_2}\cdots\mathfrak{q}_s^{a_s} = \lambda/\mu$ with integers λ, μ in K such that $(\lambda, \prod_{i=1}^{s} p_i) = (\mu, \prod_{i=1}^{s} p_i) = 1$. Taking the norms of the both sides we have, by Lemmas 2 and 3,

$$q_1^{a_1}q_2^{a_2}\cdots q_s^{a_s} \equiv z_i^{\,n} \pmod{p_i}$$

for $1 \leqslant i \leqslant s$, where $z_i \in \mathbf{Z}$. Hence, as $(q_j, p_i) = 1$, we have

$$q_i^{a_i} \equiv \Big(\prod_{j\neq i} q_j^{a_j}\Big)^{-1} z_i^{\,n} \pmod{p_i}$$

and so, by (7),

$$r_i^{a_i} \equiv \Big(\prod_{j\neq i} r_i^{a_j}\Big)^{-t_i} z_i^{\,n} \pmod{p_i}.$$

Then we have

$$\begin{aligned} r_i^{a_i(p_i-1)/t_i} &\equiv \Big(\prod_{j\neq i} r_i^{a_j}\Big)^{-t_i(p_i-1)/t_i} z_i^{\,n(p_i-1)/t_i} \\ &\equiv 1 \pmod{p_i}, \end{aligned}$$

which implies that t_i divides a_i $(1 \leqslant i \leqslant s)$.

Now let $X = [X_1] \times [X_2] \times \cdots \times [X_s]$ be a free abelian group generated by s elements $X_1, X_2, \ldots, X_s$. There exists a surjective homomorphism of X onto the subgroup, generated by $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_s$, of C_K such that $X_i \to \mathfrak{C}_i$ for $1 \leqslant i \leqslant s$. Then the above arguments show that the kernel of this homomorphism is contained in

$$[X_1^{t_1}] \times [X_2^{t_2}] \times \cdots \times [X_s^{t_s}],$$

which is of index $t_1 t_2 \cdots t_s$ in X. So the order of the group generated by $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_s$ is divisible by $\prod_{i=1}^{s} t_i = \prod_{i=1}^{s} (p_i - 1, n)$.

Therefore we have the following

THEOREM 2. *Let $K = \mathbf{Q}(a^{1/n})$, where n is odd. Let $p_1, p_2, \ldots, p_s$ be rational prime numbers such that $p_i^{e_i} \parallel a$ with $(e_i, n) = 1$. Then $\prod_{i=1}^{s} (p_i - 1, n)$ divides the class number h_K of K.*

Remark. If some $p_i = 2$, then $(p_i - 1, n) = 1$. So we may assume $p_i \neq 2$ in the course of the proof.

COROLLARY. *Let K' be a subfield of K (in Theorem 2), of degree n'. Then $\prod_{i=1}^{s} (p_i - 1, n')$ divides $h_{K'}$.*

Proof. By Corollary of Proposition, K' is also of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$. Using the notations in the proof of Theorem 2, we put $\mathfrak{q}_i' = \mathfrak{q}_i \cap K'$, which is a prime divisor of q_i in K', of degree 1. Let $\mathfrak{C}_i'$ be the ideal class of $\mathfrak{q}_i'$. Then, similarly as in the proof of Theorem 2, we see that

$$\mathfrak{C}_1'^{a_1}\mathfrak{C}_2'^{a_2} \cdots \mathfrak{C}_s'^{a_s} = 1 \text{ in } C_{K'} \text{ implies}$$

$$r_i^{a_i} \equiv \Big(\prod_{j \neq i} r_i^{a_j}\Big)^{-t_i} z_i'^{n'} \pmod{p_i} \qquad \text{with} \quad z_i' \in \mathbf{Z}.$$

As $t_i' = (p_i - 1, n') \mid t_i = (p_i - 1, n)$, we have

$$r_i^{a_i(p_i-1)/t_i'} \equiv 1 \pmod{p_i} \quad \text{and so} \quad t_i' \mid a_i \quad (1 \leqslant i \leqslant s).$$

So the order of the group generated by $\mathfrak{C}_1', \mathfrak{C}_2', \ldots, \mathfrak{C}_s'$ is divisible by $\prod_{i=1}^{s} (p_i - 1, n')$.

B. *The Case of Even n*

For an odd prime divisor p of a, let $2t = (p - 1, 2n)$. Clearly we have

$$\begin{aligned} &t \text{ is even if } p \equiv 1 \pmod 4, \\ &t \text{ is odd if } p \equiv 3 \pmod 4. \end{aligned} \tag{8}$$

We can take prime numbers $q_1, q_2, \ldots, q_s$ such that

$$\begin{gathered} q_i \nmid na, \qquad (q_i - 1, n) = 2, \\ q_i \equiv \begin{cases} r_i^2 \pmod{p_i} & \text{if} \quad p_i \equiv 1 \pmod 4, \\ r_i \pmod{p_i} & \text{if} \quad p_i \equiv 3 \pmod 4, \end{cases} \\ q_i \equiv r_j^{t_j} \pmod{p_j} \qquad \text{for} \quad j \neq i, \\ \left(\frac{a}{q_i}\right) = 1, \end{gathered} \tag{9}$$

where $2t_j = (p_j - 1, 2n)$. In fact, we can find such a q_i in the arithmetic progression defined by

$$\begin{gathered} q_i \equiv 7 \pmod 8, \\ q_i \equiv \begin{cases} r_i^2 \pmod{p_i} & \text{if} \quad p_i \equiv 1 \pmod 4, \\ r_i \pmod{p_i} & \text{if} \quad p_i \equiv 3 \pmod 4, \end{cases} \\ q_i \equiv r_j^{t_j} \pmod{p_j} \qquad \text{for} \quad j \neq i, \\ q_i \equiv r^t \pmod p \qquad \text{for odd prime divisors } p \text{ of } a \ (\neq p_1, \ldots, p_s) \end{gathered}$$

where r = a primitive root modulo p,

$$q_i \equiv 2 \pmod{p'} \qquad \text{for odd prime divisors } p' \text{ of } n \ (p' \nmid a).$$

Here we note that, as $2t \mid (p-1)$, $t < p-1$ and so $r^t \not\equiv 1 \pmod{p}$. As $\left(\frac{2}{q_i}\right) = 1$, we have

$$\left(\frac{a}{q_i}\right) = \prod \left(\frac{p}{q_i}\right) = \prod (-1)^{\frac{1}{2}(p-1)} \left(\frac{q_i}{p}\right) = 1,$$

where the product ranges over all the odd prime divisors p of a such that $p^{\text{odd}} \| a$. Now, as $\left(\frac{a}{q_i}\right) = 1$, we have $y^2 \equiv a \pmod{q_i}$ with some $y \in \mathbf{Z}$. Moreover, by $(q_i - 1, n) = 2$, we have also $x^n \equiv y^2 \pmod{q_i}$ with some $x \in \mathbf{Z}$ and so the polynomial $X^n - a \pmod{q_i}$ has a root in $\mathbf{Z}/(q_i)$. So, by $q_i \nmid na$, there is a prime divisor $\mathfrak{q}_i$ of q_i, of degree 1, in K. Let $\mathfrak{C}_i$ be the ideal class of $\mathfrak{q}_i$ in C_K. Suppose that we have

$$\mathfrak{C}_1^{a_1} \mathfrak{C}_2^{a_2} \cdots \mathfrak{C}_s^{a_s} = 1 \text{ in } C_K.$$

Then, similarly as in Section A, we have

$$q_i^{a_i} \equiv \pm \left(\prod_{j \neq i} q_j^{a_j} \right)^{-1} z_i^{\,n} \pmod{p_i}$$

for $1 \leqslant i \leqslant s$, where $z_i \in \mathbf{Z}$. So, by (9), we have

$$r_i^{k_i a_i} \equiv \pm \left(\prod_{j \neq i} r_i^{a_j} \right)^{-t_i} z_i^{\,n} \pmod{p_i},$$

where $k_i = 2$ or 1 according as $p_i \equiv 1$ or $3 \pmod 4$, i.e., $k_i = (2, t_i)$. Then we have, as $(p_i - 1)/t_i$ is even and $t_i \mid n$,

$$\begin{aligned} r_i^{k_i a_i (p_i - 1)/t_i} &\equiv \left(\prod_{j \neq i} r_i^{a_j} \right)^{-t_i (p_i - 1)/t_i} z_i^{n(p_i - 1)/t_i} \\ &\equiv 1 \pmod{p_i}, \end{aligned}$$

which implies that t_i divides $k_i a_i$, i.e., $t_i/(2, t_i)$ divides a_i $(1 \leqslant i \leqslant s)$.

Therefore, from similar arguments as in Section A, we have the following

THEOREM 3. *Let $K = \mathbf{Q}(a^{1/n})$, where n is even. Let $p_1, p_2, \ldots, p_s$ be odd rational prime numbers such that $p_i^{e_i} \| a$ with $(e_i, n) = 1$. Then $\prod_{i=1}^{s} t_i/(2, t_i)$ divides the class number h_K of K, where $2t_i = (p_i - 1, 2n)$.*

COROLLARY. *Let K' be a subfield of K (in Theorem 3), of degree n'. If n' is odd then $\prod_{i=1}^{s}(p_i - 1, n')$ divides $h_{K'}$. If n' is even then $\prod_{i=1}^{s} t_i'/(2, t_i')$ divides $h_{K'}$, where $2t_i' = (p_i - 1, 2n')$.*

Proof. We use the notations in the proof of Theorem 3. Similarly as in the proof of the Corollary to Theorem 2, K' is of Eisenstein type with respect to $p_1, p_2, \ldots, p_s$ and q_i has a prime divisor $\mathfrak{q}_i'$ in K', of degree 1. Let $\mathfrak{C}_i'$ be the ideal class of $\mathfrak{q}_i'$. If n' is odd, $\mathfrak{C}_1'^{a_1}\mathfrak{C}_2'^{a_2} \cdots \mathfrak{C}_s'^{a_s} = 1$ in $C_{K'}$ implies

$$r_i^{k_i a_i} \equiv \Big(\prod_{j \neq i} r_i^{a_j}\Big)^{-t_i} z_i'^{n'} \pmod{p_i}$$

with $z_i' \in \mathbf{Z}$. As $(p_i - 1, n')$ is odd and so $(p_i - 1, n') \mid t_i = (p_i - 1, n)/2$, we see $(p_i - 1, n') \mid k_i a_i$, i.e. $(p_i - 1, n') \mid a_i$ for $1 \leqslant i \leqslant s$. If n' is even, $\mathfrak{C}_1'^{a_1}\mathfrak{C}_2'^{a_2} \cdots \mathfrak{C}_s'^{a_s} = 1$ in $C_{K'}$ implies

$$r_i^{k_i a_i} \equiv \Big(\prod_{j \neq i} r_i^{a_j}\Big)^{-t_i} (\pm z_i'^{n'}) \pmod{p_i}$$

with $z_i' \in \mathbf{Z}$. As $2t_i' = (p_i - 1, 2n') \mid 2t_i = (p_i - 1, 2n)$, i.e., $t_i' \mid t_i$, $(p_i - 1)/t_i'$ is even and $t_i' \mid n'$, we see that t_i' divides $k_i a_i$. We have easily $k_i = (2, t_i')$ and so $t_i'/(2, t_i') \mid a_i$ for $1 \leqslant i \leqslant s$. Then the assertions of the Corollary follows similarly as in the proof of Theorem 2.